



## Safer Internet Day Open House

The Protection of Privately Identifiable Information and Passwords  
on the Internet

Thursday, 21 March, 13

Welcome:

- Really appreciate you taking the time out of your day to join us for this event! We are really excited to share some thoughts and ideas with you that we believe will really benefit you and your home in making your internet experiences safer!

This session we are going to talk about how to keep your personal information safe on the web. Hopefully we will discuss some topics and strategies that may be new to you.

To begin, I'm going to play you a short video of a social encounter. I'd like you to jot down anything that you believe could be personally identifiable information.



Social Media = Social Conversation



# Protecting PII and Passwords

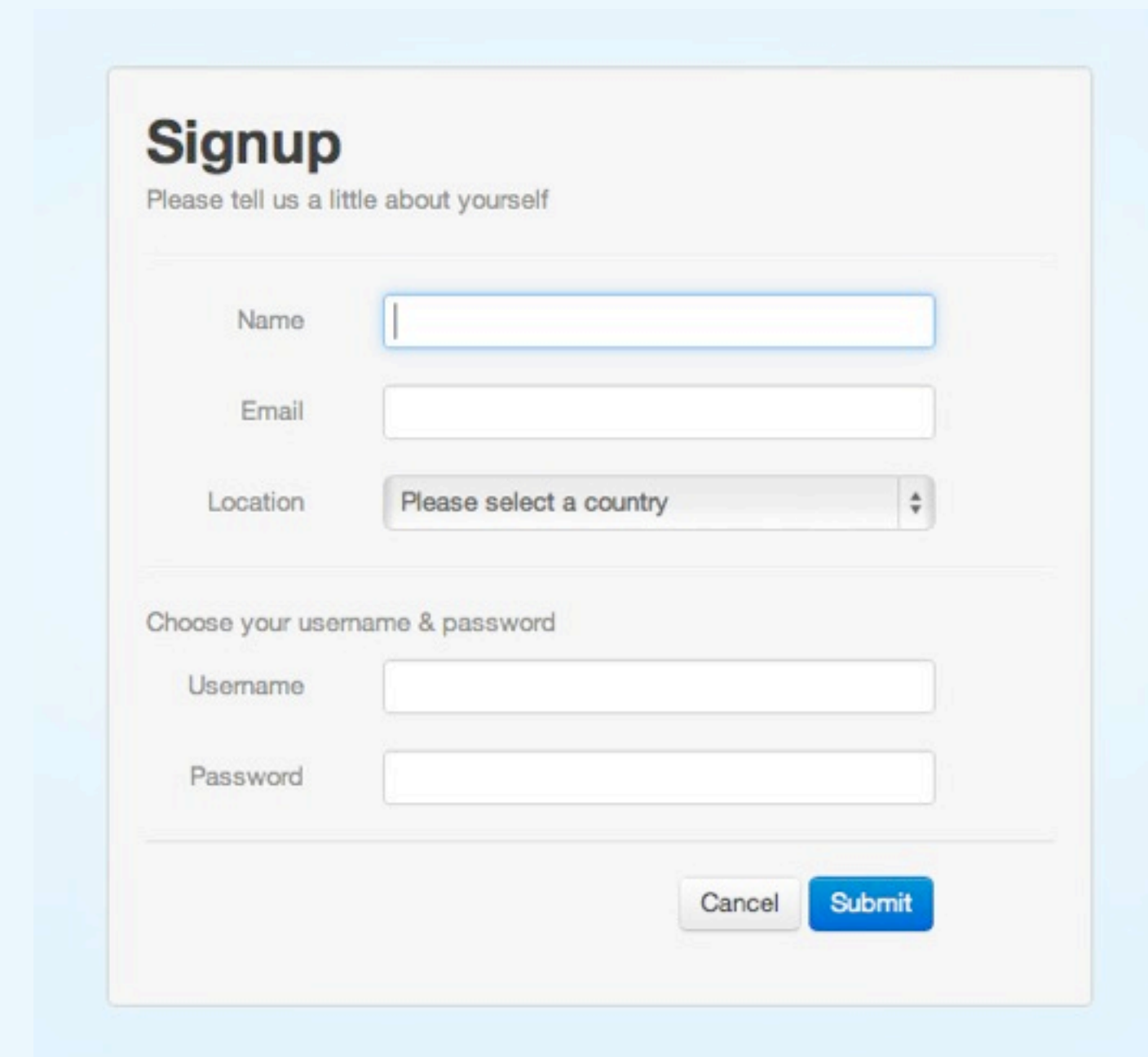


Social Media = Social Conversation



## Starting the Conversation: Accounts & Passwords:

- Account creation
  - Use an alias
- Password creation
  - Password sharing
- Emails
  - Personal email and social media email
- Security questions
  - Avoid common personal information
- Rule of 10,000
  - Does this narrow you down?





## Sites: What's in your control?



- Security settings
  - Who is this conversation with?
- Geo-tagging
  - Where are you posting from?
- Logging out of your account
  - Unwanted access
- Password protect your wifi
  - Leaving your information open



### SECURITY SETTINGS:

- Any social media site asking for your personal information will give you the option to display this information on your page. The ability to turn this on and off is completely in your control. Note most site that ask this will automatically display the information unless you turn it off. These settings can change per site; however, most are found with your account information or security settings
- Approval settings

### GEO-TAGGING:

- It's becoming more and more common to geo-tag where you are posting from. Meaning, if you attend a soccer game in east kelowna, take a photo and post it to social media your photo will be tagged with a generalized location.
- When posting from a mobile: If the location you are posting from is a known location, such as a Starbucks or something searchable on your google maps, the information can display automatically if not other wise selected

### LOGGING OUT OF YOUR ACCOUNT:

- May seem like the simplest action to protect personal information, but is often the first and most common way to gain access to other's personal information. Removing the 'remember me' feature on mobile devices or password protecting simple apps is an easy way to protect your information

### PASSWORD PROTECT YOUR WIFI:

- Passwords are the simplest ways to monitor when people or family members are using your internet. Additionally, this prevents people from outside your network from accessing your information.

## Sites: What's in your control?



- Security settings
  - Who is this conversation with?
- Geo-tagging
  - Where are you posting from?
- Logging out of your account
  - Unwanted access
- Password protect your wifi
  - Leaving your information open



Like · Comment · Share · 2 minutes ago near Kelowna ·

### SECURITY SETTINGS:

- Any social media site asking for your personal information will give you the option to display this information on your page. The ability to turn this on and off is completely in your control. Note most site that ask this will automatically display the information unless you turn it off. These settings can change per site; however, most are found with your account information or security settings
- Approval settings

### GEO-TAGGING:

- It's becoming more and more common to geo-tag where you are posting from. Meaning, if you attend a soccer game in east kelowna, take a photo and post it to social media your photo will be tagged with a generalized location.
- When posting from a mobile: If the location you are posting from is a known location, such as a Starbucks or something searchable on your google maps, the information can display automatically if not other wise selected

### LOGGING OUT OF YOUR ACCOUNT:

- May seem like the simplest action to protect personal information, but is often the first and most common way to gain access to other's personal information. Removing the 'remember me' feature on mobile devices or password protecting simple apps is an easy way to protect your information

### PASSWORD PROTECT YOUR WIFI:

- Passwords are the simplest ways to monitor when people or family members are using your internet. Additionally, this prevents people from outside your network from accessing your information.



## What's next? Keep an Open Dialogue:



PARENTS CAN PLAY TOO:  
- Getting involved in your child's online time is the best way to show interest in what they are doing whilst being able to monitor their online activity.  
- Perhaps challenge them to a duel or game  
- Create an avatar yourself and ask them to show you around

DON'T BE THE LAST TO KNOW:  
Getting involved can also allow you to move up the ladder in communication. More often than not parents can be the last ones to know about an uncomfortable encounter online; however, if you are involved in what they are doing, they may be more likely to let you in on situations, asking for your help. Parents are the safest place for a child and opening up communication in more areas of a child's life only broadens those communication levels  
- If an unsafe encounter happens your child is more likely to let you know about what happened in that environment, because you ARE a part of that environment

HOW TO TALK TO STRANGERS:  
- Much like 'don't talk to strangers' in the real world similar boundaries need to be set up online. However, instead of 'Don't talk to strangers' as a general rule, teaching your child HOW to talk to strangers can be a more useful tool. After all, most people online are strangers.  
- If you teach a child to NEVER talk to strangers, they won't know how to actually react when they encounter one. Establishing rules as to what is personal information and what is not can be a better way to educate your child on how to keep them safe, rather than trying to keep them from all unsafe situations.  
- Much like a self defence class, learning how to protect yourself physically, kids need a self defence class for the web. What would this look like in your home? Develop one together with your kids. Propose your guidelines and ideas and have them retort with their own thoughts.  
- Ask questions such as, Does this information narrow you down to a pool of less than 10,000 people??

DON'T PULL THE PLUG:  
- In today's day and age kids often know more than the parents when it comes to navigating technology. Pulling the plug or completely eliminating access to the web can be a very dangerous move.  
- To a teen or child accessing the web can then become an enticing act of rebellion.  
- With wifi, gaming systems, phones, tablets, laptops, school computer labs, public libraries even stores such as Best Buy, when displaying computers that are for sale offer very easy paths to the internet  
- The answer is not removing this freedom, but opening up conversation about this privilege. Learning what's out there, what your kids like and what is your role within it?



## What's next? Keep an Open Dialogue:

- Parents can play too



PARENTS CAN PLAY TOO:  
- Getting involved in your child's online time is the best way to show interest in what they are doing whilst being able to monitor their online activity.  
- Perhaps challenge them to a duel or game  
- Create an avatar yourself and ask them to show you around

DON'T BE THE LAST TO KNOW:  
Getting involved can also allow you to move up the ladder in communication. More often than not parents can be the last ones to know about an uncomfortable encounter online; however, if you are involved in what they are doing, they may be more likely to let you in on situations, asking for your help. Parents are the safest place for a child and opening up communication in more areas of a child's life only broadens those communication levels  
- If an unsafe encounter happens your child is more likely to let you know about what happened in that environment, because you ARE a part of that environment

HOW TO TALK TO STRANGERS:  
- Much like 'don't talk to strangers' in the real world similar boundaries need to be set up online. However, instead of 'Don't talk to strangers' as a general rule, teaching your child HOW to talk to strangers can be a more useful tool. After all, most people online are strangers.  
- If you teach a child to NEVER talk to strangers, they won't know how to actually react when they encounter one. Establishing rules as to what is personal information and what is not can be a better way to educate your child on how to keep them safe, rather than trying to keep them from all unsafe situations.  
- Much like a self defence class, learning how to protect yourself physically, kids need a self defence class for the web. What would this look like in your home? Develop one together with your kids. Propose your guidelines and ideas and have them retort with their own thoughts.  
- Ask questions such as, Does this information narrow you down to a pool of less than 10,000 people??

DON'T PULL THE PLUG:  
- In today's day and age kids often know more than the parents when it comes to navigating technology. Pulling the plug or completely eliminating access to the web can be a very dangerous move.  
- To a teen or child accessing the web can then become an enticing act of rebellion.  
- With wifi, gaming systems, phones, tablets, laptops, school computer labs, public libraries even stores such as Best Buy, when displaying computers that are for sale offer very easy paths to the internet  
- The answer is not removing this freedom, but opening up conversation about this privilege. Learning what's out there, what your kids like and what is your role within it?

## What's next? Keep an Open Dialogue:

- Parents can play too
- Don't be the last to know



## What's next? Keep an Open Dialogue:

- Parents can play too
- Don't be the last to know
- How to talk to strangers



**PARENTS CAN PLAY TOO:**  
- Getting involved in your child's online time is the best way to show interest in what they are doing whilst being able to monitor their online activity.  
- Perhaps challenge them to a duel or game  
- Create an avatar yourself and ask them to show you around

**DON'T BE THE LAST TO KNOW:**  
Getting involved can also allow you to move up the ladder in communication. More often than not parents can be the last ones to know about an uncomfortable encounter online; however, if you are involved in what they are doing, they may be more likely to let you in on situations, asking for your help. Parents are the safest place for a child and opening up communication in more areas of a child's life only broadens those communication levels  
- If an unsafe encounter happens your child is more likely to let you know about what happened in that environment, because you ARE a part of that environment

**HOW TO TALK TO STRANGERS:**  
- Much like 'don't talk to strangers' in the real world similar boundaries need to be set up online. However, instead of 'Don't talk to strangers' as a general rule, teaching your child HOW to talk to strangers can be a more useful tool. After all, most people online are strangers.  
- If you teach a child to NEVER talk to strangers, they won't know how to actually react when they encounter one. Establishing rules as to what is personal information and what is not can be a better way to educate your child on how to keep them safe, rather than trying to keep them from all unsafe situations.  
- Much like a self defence class, learning how to protect yourself physically, kids need a self defence class for the web. What would this look like in your home? Develop one together with your kids. Propose your guidelines and ideas and have them retort with their own thoughts.  
- Ask questions such as, Does this information narrow you down to a pool of less than 10,000 people??

**DON'T PULL THE PLUG:**  
- In today's day and age kids often know more than the parents when it comes to navigating technology. Pulling the plug or completely eliminating access to the web can be a very dangerous move.  
- To a teen or child accessing the web can then become an enticing act of rebellion.  
- With wifi, gaming systems, phones, tablets, laptops, school computer labs, public libraries even stores such as Best Buy, when displaying computers that are for sale offer very easy paths to the internet  
- The answer is not removing this freedom, but opening up conversation about this privilege. Learning what's out there, what your kids like and what is your role within it?



## What's next? Keep an Open Dialogue:

- Parents can play too
- Don't be the last to know
- How to talk to strangers
- Don't pull the plug



# Protecting PII and Passwords





## Safer Internet Day Open House

The Protection of Privately Identifiable Information and Passwords  
on the Internet

Thursday, 21 March, 13

Welcome:

- Really appreciate you taking the time out of your day to join us for this event! We are really excited to share some thoughts and ideas with you that we believe will really benefit you and your home in making your internet experiences safer!

This session we are going to talk about how to keep your personal information safe on the web. Hopefully we will discuss some topics and strategies that may be new to you.

To begin, I'm going to play you a short video of a social encounter. I'd like you to jot down anything that you believe could be personally identifiable information.